IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN RE: CAPITAL ONE CONSUMER DATA SECURITY BREACH LITIGATION	MDL No. 1:19md2915 (AJT/JFA)

This Document Relates to the Consumer Cases

MEMORANDUM IN SUPPORT OF PLAINTIFFS' MOTION TO COMPEL DISCOVERY FROM AMAZON DEFENDANTS

Plaintiffs submit this Memorandum in Support of their Motion to Compel Amazon's Response to Request for Production of Document No. 14, Answers to Interrogatories 8 and 17, and deposition testimony responsive to Areas of Inquiry 21 and 26 of Plaintiff's Fed. R. Civ. P. 30(b)(6) deposition notice (collectively, the "Contested Amazon Discovery").

Particular to this Motion, the Contested Amazon Discovery can be distilled into two overarching areas of inquiry: 1) Amazon's knowledge of issues or vulnerabilities related to misconfigured WAFs, SSRF Attacks, open reverse proxy attacks, and overly broad IAM permissions from sources other than the Capital One Data Breach; and 2) the financial benefits Amazon received from Capital One's cloud environment, including Capital One's customers' data, and/or Capital One's PII data stored in its data lake.

PRELIMINARY STATEMENT

On July 29, 2019, Capital One announced it had experienced a data breach that affected over 100 million people in the United States and six million people in Canada (the "Data Breach"). Corrected Representative Consumer Class Action Complaint ("Complaint" or "Compl."), Dkt. 354, at ¶¶ 1–2.

According to Capital One, the intrusion occurred through a misconfigured firewall that Capital One was using as a part of its operations that were hosted on the public cloud service of Defendant Amazon Web Services, Inc. ("AWS"), a subsidiary of Defendant Amazon.com, Inc. (collectively, "Amazon"). AWS hosts and runs public cloud services that are leased to companies such as Defendants Capital One Financial Corporation, Capital One, N.A., and Capital One Bank (USA), N.A. (collectively, "Capital One"). Compl. ¶ 37. The benefit of hosting data on a public cloud service is that companies can save money by paying for only the computing power and storage they need, rather than maintaining a dedicated server or private cloud. *Id.* The downside is the increased data security risks inherent in the use of public cloud computing. *Id.* ¶ 38. For this reason, banks have historically been reticent to use public cloud services. *Id.*

Plaintiffs served discovery on Amazon seeking, *inter alia*, relevant information concerning: 1) Amazon's security configurations (*i.e.*, WAFs), knowledge of attacks (*i.e.*, SSRF and open proxy attacks), and overly broad IAMs; and 2) the financial benefits Amazon received regarding Capital One, Capital One's customers' data, and/or Capital One's PII data stored in its data lake. Amazon objected, claiming these issues are outside the scope of permissible discovery, and Amazon has refused to further respond to the Contested Amazon Discovery: Amazon will not provide any further responses to interrogatories, produce documents, or produce witnesses under Rule 30(b)(6) on the Contested Amazon Discovery. These discovery requests are clearly relevant to this litigation and the Court should find accordingly.

In light of the arguments detailed herein, the Court should find the Contested Amazon Discovery is relevant, and order Amazon to substantively and meaningfully respond to the Contested Amazon Discovery. Specifically, Plaintiffs seek: (1) answers to interrogatories; (2)

production of documents; and (3) designated witness(es) competent and knowledgeable to testify regarding the Contested Amazon Discovery.

BACKGROUND

A. Amazon's Culpability for the Data Breach

Despite the inherent security risks described above with moving information to the public cloud (*i.e.*, increased data security risks inherent in the use of public cloud computing), in 2015, Capital One announced that it would move all of its data to the public cloud, and in 2016, it announced that AWS would be its predominant public cloud provider. *Id.* ¶ 39. Choosing to place its data on the public cloud was an aggressive move into uncharted territory for a major bank and meant that Capital One's customer data would no longer be in its physical custody, but instead in the hands of a third-party partner. *Id.* ¶ 41. For its part, Amazon touted the AWS cloud environment as a technology-forward solution for Capital One's aggressive data collection strategy. Partnering with AWS allowed Capital One to use Amazon's data scientists and artificial intelligence to analyze the data it collected from credit applicants as part of Capital One's push to become a "technology company." *Id.* ¶¶ 32–33, 40.

Aware of the risks of the move to public cloud services, both Capital One and its partner Amazon needed to convince customers that information stored in the AWS cloud environment would be safe. Accordingly, both Capital One and AWS began making deceptive, false, misleading, and unfair representations regarding the security of the customer data being stored on the cloud. *Id.* ¶ 42. For instance, in October 2015, at an Amazon-sponsored industry event known as "AWS re:Invent 2015," Capital One's Chief Information Officer used his keynote address to announce that Capital One was shifting its data to the cloud. In those remarks he stated: "[S]ecurity is critical for us. The financial services industry attracts some of the worst cyber criminals so we

work closely with the Amazon team to develop a security model which we believe enables us to operate more securely in the public cloud than we can even in our own data centers." *Id.* ¶ 44.

Despite these public assurances about their commitment to data security, both Capital One and AWS were aware of data security vulnerabilities in the AWS cloud environment. *Id.* ¶ 45. In fact, these vulnerabilities were well-known in the cloud computing industry. *Id.* ¶ 54. Unlike servers run by AWS competitors Google and Microsoft, AWS servers were not secured against SSRF attacks, which allow an intruder to penetrate a firewall and exfiltrate data to a third-party server. *Id.* ¶ 46. The firewalls on the AWS cloud are known to be vulnerable to an SSRF attack.[1] In an SSRF attack, an attacker tricks a server into thinking that the attacker is permitted to request and access data. By tricking a server into thinking that it is receiving a legitimate request from inside the firewall (rather than an illegitimate request from outside), the attacker obtains a foothold inside the network. *Id.* ¶ 52.

Despite this being a well-known problem exploited by hackers, AWS has no protections built into its systems to protect against an SSRF attack. *Id.* ¶ 53. Year after year, this known flaw was the subject of presentations at some of the largest cybersecurity conferences in the United States. *Id.* ¶ 46. According to Evan Johnson, manager of the product security team at Cloudflare, "SSRF has become the most serious vulnerability facing organizations that use public clouds . . . . The impact of SSRF is being worsened by the offering of public clouds, and the major players like AWS are not doing anything to fix it. The problem is common and well-known, but hard to prevent and does not have any mitigations built into the AWS platform." *Id.* ¶ 55. In contrast to AWS, Google and Microsoft built protections against SSRF attacks. *Id.* ¶ 54.

---

[1] The precise technical details of the permissions that allow the AWS servers to pull data and facilitate machine learning are set forth in paragraphs 47-53 of the Complaint.

AWS and Capital One publicly acknowledged the SSRF vulnerabilities in AWS's cloud computing services in 2016, when they jointly announced that together they had developed a new product called Cloud Custodian. They announced that with Cloud Custodian they had solved the security problems inherent in using the AWS cloud for machine learning, characterizing Cloud Custodian as a comprehensive cloud security tool that would automatically detect and fix security flaws. *Id.* ¶ 56. They represented that Cloud Custodian would, among other things, automatically scan Capital One's internal systems to ensure that all of the servers and permissions were set according to defined policies and automatically encrypt all data on the AWS servers. *Id.* ¶¶ 57–58. However, encrypting the data stored on the AWS servers did not solve the security vulnerability. An intruder able to get past the firewall could decrypt the data on the server. *Id.* ¶ 58.

At Amazon's yearly re:Invent conference in November 2018, Capital One's Senior Distinguished Engineer Kapil Thangavelu gave a presentation describing the precise vulnerability in the AWS cloud service that would ultimately result in the Data Breach. *Id.* ¶ 59. Based on his comments, it is clear that Capital One and Amazon appreciated the risk that someone who could breach the firewall could gain full access to the data stored on an AWS server. It was this known vulnerability that allowed a former "systems engineer" for AWS (*id.* ¶ 63) to steal Capital One's customer data in March 2019. Despite its knowledge of this vulnerability, AWS failed to take the appropriate steps—or any steps at all—to protect Plaintiffs' and the class members' PII.

B. Plaintiffs' Discovery Requests and Amazon's Objections and Lack of Substantive Responses to the Contested Amazon Discovery

On January 31, 2020, Plaintiffs served Amazon with their First Request for Production of Documents, First Interrogatories, and Notice of Rule 30(b)(6) Deposition (the "Amazon Discovery Requests"). On February 18, 2020, Amazon served its objections to the Amazon Discovery Requests, and on February 24, 2020, Plaintiffs' counsel requested a meet and confer to discuss the

objections in advance of the March 2, 2020 deadline for Amazon's responses to the Amazon Discovery Requests; the parties met and conferred on February 27, 2020 without substantial resolution of the Contested Amazon Discovery. On March 2, 2020, Amazon produced approximately 77 documents but stood (and to this day stands) on its objections to the Contested Amazon Discovery as beyond the permissible scope of discovery in this case. Copies of Amazon's respective responses to Plaintiffs' Amazon Discovery Requests are attached hereto as Exhibits A (Objections to Plaintiffs' First Request for Production of Documents), B (Objections and Responses to Plaintiffs' First Interrogatories), and C (Objections to Plaintiffs' Notice of Videotaped Depositions).

Particular to this Motion, the two overarching disputed areas of inquiry are: 1) Amazon's knowledge of issues or vulnerabilities related to misconfigured WAFs, SSRF Attacks, open reverse proxy attacks, and overly broad IAM permissions acquired outside of the Capital One Data Breach; and 2) the financial benefits Amazon has received from Capital One's cloud environment, including Capital One's customers' data, and/or Capital One's PII data stored in its data lake. *See, e.g.*, Ex. A, Request 14; Ex. B, Interrogatories 8, 17; Ex. C, Topics 21, 26.

C. Efforts to Resolve the Discovery Disputes

i. Correspondences between February and April 2020

In accord with Local Civil Rule 37, on February 27, 2020, Plaintiff's counsel met and conferred in good faith with Amazon's counsel to resolve disputes with search terms and Amazon's compliance with the Court's Order Adopting Search Term Protocol, (Dkt. 330), concerning the Contested Amazon Discovery. *See* Correspondences with Counsel, a true and correct copy of which is attached hereto as Exhibit D. Following that conference, and several follow up communications, Plaintiffs' counsel provided a deficiency letter concerning Amazon's discovery responses, including the Contested Amazon Discovery at issue in this Motion. *See* Ex.

D, p. 1; *see generally* April 17, 2020 Deficiency Letter, a true and correct copy of which is attached hereto as Exhibit E.

ii. The April 17, 2020 Deficiency Letter and Subsequent Meet and Confers

In its April 17, 2020 Deficiency Letter, Plaintiffs' counsel outlined the deficiencies in Amazon's Responses to Plaintiffs' First Interrogatories. *See generally*, Ex. E. Plaintiffs' counsel also expressed the unsatisfactory nature of Amazon's Responses to Plaintiffs' First Requests for Production. *See* Ex. E, p. 1 (noting that "While Amazon's Responses to Plaintiffs' First Requests for Production suffer from similar flaws, we hope the issues discussed herein will resolve most of those issues as well, without need for separate extended correspondence."). Following the April 17, 2020 Deficiency Letter, counsel for Plaintiffs and Amazon scheduled a meet and confer for Wednesday, April 22, 2020. *See* April 24, 2020 Correspondence, a true and correct copy of which is attached hereto as Exhibit F. During the April 22, 2020 meet and confer, Amazon's Counsel represented they could not estimate any volume of documents that might be collected from likely custodians, and did not have any estimated turn-around time for providing any documents responsive to the Amazon Discovery Requests. *See* Ex. F, p. 2. Essentially, Amazon did not perform any substantive or meaningful actions to investigate the Amazon Discovery Requests—it had not identified documents, and certainly had not begun any meaningful review or processing of documents identified as potentially responsive to the Contested Amazon Discovery. *See* Ex. F, pp. 1–2.

iii. The Contested Amazon Discovery Remains Unresolved

Although the parties met and conferred on May 1, 2020, to discuss *inter alia* the Contested Amazon Discovery—including witnesses designated under Rule 30(b)(6)—Amazon remains steadfast in its assertion that discovery related to Amazon's knowledge of issues or vulnerabilities related to misconfigured WAFs, SSRF Attacks, open reverse proxy attacks, and overly broad IAM

permissions beyond any knowledge gained as a result of the Capital One Data Breach; and the financial benefits Amazon received from Capital One's cloud environment, including Capital One's customers' data, and/or Capital One's PII data stored in its data lake, is irrelevant and beyond the permissible scope of discovery in this case. Plaintiffs strongly disagree, and for the reasons argued herein, implore this Court for an Order requiring Amazon to substantively and meaningfully respond to the Contested Amazon Discovery to the full extent contemplated by the applicable Federal Rules of Civil Procedure.

LEGAL STANDARD

"Parties are entitled to discover any material that is relevant to any party's claim or defense, is nonprivileged, and proportional to the needs of the case." *BASF Plant Sci., LP v. Commonwealth Sci. and Indus. Research Org.*, No. 2:17-cv-503, 2019 WL 8108060 (E.D. Va. July 3, 2019) (Morgan, J.) (citing Fed. R. Civ. P. 26(b)(1)). Relevance in this context is to be read liberally. *Id.*; Fed. R. Civ. P. 26(b)(1) ("Information within this scope of discovery need not be admissible in evidence to be discoverable). Proportionality considers: "the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. *Ibid.* Accordingly, "[t]he Federal Rules contemplate the broadest discovery possible in the search for the truth." *Id.* (quoting *Doe v. Old Dominion Univ.*, 289 F.Supp.3d 744, 749 (E.D. Va. 2018) (Morgan, J.)); *see Seldowitz v. Office of Inspector Gen. U.S. Dept. of State*, 238 F.3d 414 (Table), 2000 WL 1742098, at *5 (4th Cir. Nov. 13, 2000); *Minor v. Bostwick Lab's, Inc.*, No. 3:09-cv-343, 2012 WL 13028138 (E.D. Va. July 13, 2012) (Novak, J.).

"Pursuant to Federal Rule of Civil Procedure 37(a), a party may move for an order compelling disclosure or discovery. Fed. R. Civ. P. 37. Local Rule 37(A) further provides: 'After a discovery request is objected to, or not complied with, within time, and if not otherwise resolved, it is the responsibility of the party initiating discovery to place the matter before the court by a proper motion…to compel an answer, production, designation, or inspection.'" *Addax Energy SA v. M/V Yasa H. Mulla*, No. 2:17-cv-641, 2018 WL 10470917, at *3 (E.D. Va. Nov. 13, 2018) (Morgan, J.) (marks in original). The Court is afforded broad discretion in this regard. *Rowland v. Am. Gen. Fin., Inc.*, 340 F.3d 187, 195 (4th Cir. 2003); *Lone Star Steakhouse & Saloon, Inc. v. Alpha of Va.*, 43 F.3d 416, 426 (4th Cir. 1996); *Wu v. Tseng*, No. 2:06-cv-346, 2007 WL 4143077, at *3 (E.D. Va. Nov. 19, 2007) (Morgan, J.).

"[T]he party or person resisting discovery, not the party moving to compel discovery, bears the burden of persuasion." *Addax Energy*, 2018 WL 10470917, at *4 (quoting *Eramo v. Rolling Stone, LLC*, 314 F.R.D. 205, 209 (W.D. Va. 2016) (Conrad, J.) (marks in original); *Old Dominion*, 289 F.Supp.3d at 749. Particularly when electronically stored information ("ESI") is implicated, "the party resisting its production must show that the ESI is not reasonably accessible due to burden or cost, and, even if such a showing is made, the Court may nevertheless order its production if the requesting party shows good cause, keeping in mind Rule 26(a)(2)(C). *Id.*

ARGUMENT

A. The Contested Amazon Discovery is Highly Relevant to this Litigation

i. Discovery related to WAFs, SSRF and open reverse proxy attacks, and overly broad IAM permissions is directly at issue and relevant to this litigation

Evidence of Amazon's lackadaisical security and treatment of vulnerabilities in its WAFs, treatment of SSRF and open reverse proxy attacks, ill-permissioned IAMs, and other crucial vulnerabilities has already been produced in this litigation—but not by Amazon. In its rolling

production, Capital One produced a document designated Confidential – Outside Counsel Only, [redacted] CapitalOne_MDL_000284977, a true and correct copy of which is attached hereto as Exhibit G. The discussion continues, acknowledging [redacted] Ex. G. Shockingly, the individuals state [redacted] Ex. G pp. 1–2. Most damning, the individuals conclude that [redacted]. Ex. G p. 3.

Indeed, Capital One [redacted] *See* Ex. E p.7. In further confirmation, Amazon acknowledged to Senator Wyden that the Data Breach occurred, at least in part, due to an open reverse proxy attack. AWS_CAP00000012, a true and correct copy of which is attached hereto as Exhibit H. Explaining in further detail, Amazon represented to Senator Wyden that "During an open reverse proxy attack, the attacker *takes advantage of a misconfigured resource, such as a web application firewall [WAF], that enables the attacker to directly query the internal networking resources for sensitive data*." Ex. H (emphasis added). Amazon further

described to Senator Wyden the efforts employed to remediate vulnerabilities of this sort to prevent future breaches. *See generally*, Ex. H. This demonstrates without question that Amazon has a robust understanding of how the attack took place, and specifically the vulnerabilities exploited to effectuate the attack.

Despite what has been revealed to date in Capital One's production and Amazon's thin production to date, Amazon continues to take the untenable position that such discovery of Amazon's knowledge of vulnerabilities of its cloud environment learned outside of the Capital One Data Breach is outside the scope of permissible discovery. But this knowledge is directly relevant to Plaintiffs' allegations that Amazon, and the industry, was well aware of , and even publicly discussed the vulnerabilities in the AWS cloud environment. *Compl.* ¶ ¶ 45, 46, 54, 55.

ii. Discovery related to the financial benefits Amazon received as a condition of partnering with Capital One is directly at issue and relevant to this litigation

The Complaint is replete with detailed allegations placing the financial arrangements between Amazon and Capital One relevant to this litigation and subject to discover. For example, Plaintiffs detail the synergies Amazon and Capital One hoped to achieve via their partnership of moving Capital One's data—including applicants and current and former customers—to Amazon's cloud computing services. Compl. ¶¶ 37–39. This included Amazon allowing Capital One to use Amazon's data scientists and artificial intelligence tools to analyze the trove of customer data it collected from credit applications (*i.e.*, the customer data stored in the data lake). Compl. ¶ 40. And because the data was no longer privately stored, but rather publicly held by Amazon's cloud servers, Compl. ¶ 41, Amazon's servers, artificial intelligence, machine learning, and other complex technologies were able to analyze the collected data of Capital One's customers. Compl. ¶ 47. Another example of Plaintiffs' allegations concerning the financial arrangements between Amazon and Capital One includes their 2016 announcement of the product Cloud

Custodian, which "had solved the security problems inherent in using the AWS cloud for machine learning at scaled, and [they] billed Cloud Custodian as a comprehensive cloud security tool which would automatically detect and fix security flaws." Compl. ¶ 56. There is no dispute the financial arrangements between Amazon and Capital One are a major issue in this MDL, and are thus discoverable. Plaintiffs informed Amazon of these positions in the April 17, 2020 Deficiency Letter, but Amazon continues to take the untenable position that such discovery is outside the scope of permissible discovery.

B. The Proportionality of the Contested Amazon Discovery Weighs in Favor of Compelling Production

In addition to being highly relevant to this litigation, the Contested Amazon Discovery is proportional to the needs of the case, and an examination of the considerations of proportionality leave no doubt that Plaintiffs' Motion should be granted.

i. The Contested Amazon Discovery is Central to this Litigation

Similar to the relevance of the Contested Discovery Requests, Plaintiffs' acquisition, review, analysis, and use of responses to the Contested Discovery Requests is important to this litigation. Although Amazon objects to providing any information concerning its knowledge of issues and vulnerabilities related to misconfigured WAFs, as well as SSRF attacks, open reverse proxy attacks, and overly broad IAM permissions beyond those concerning Capital One, any information of similar knowledge these issues with other clients substantially impacts Amazon's culpability in this matter. The extent of Amazon's knowledge of the susceptibility of its security and investigation of prior, similar attacks is a core issue in this litigation—both for liability and presumably Amazon's defensive position in this case. Denying Plaintiffs access to that discovery would substantially hinder and prejudice Plaintiffs from developing their case. Additionally, the synergies achieved and financial arrangements between Amazon and Capital One directly impact

the claims and defenses in this litigation, and blocking Plaintiffs from at the very least taking that discovery would unfairly prejudice their ability to develop their case and rebut any potential defenses from Amazon, such as a commonly-asserted defense that all resources—technological, financial, and otherwise—were committed to defending against the attack. The amount of money Amazon saved *and earned* due to its arrangement with Capital One is important both to Plaintiffs' claims and Defendants' potential defenses, and thus should fall within the scope of discovery in this litigation.

ii. The Amount in Controversy Weighs Heavily in Plaintiffs' Favor

This case involves one of the largest data breaches in history and concerns some of the most sensitive information a person can provide to a company: the full set of data necessary to apply for an obtain credit. It is beyond dispute that the amount in controversy is immense.

iii. The Relative Access of the Parties Weighs Heavily in Plaintiffs' Favor

The information requested in the Contested Amazon Discovery is directly within Amazon's possession, custody, and control: Amazon knows its customer base; Amazon knows the customers for which WAFs are provided; Amazon would have reports and other documentation concerning any reported attacks and the investigations and remediations performed in response thereto; and Amazon has direct access to the financial benefits it enjoyed as a result of the arrangement with Capital One. Indeed, Amazon indisputably would have the greatest access to the first category of information sought in the Contested Amazon Discovery (*i.e.*, history of misconfigured WAFs, attacks, and overly broad permissions), but Amazon would also have the greatest access to the second category of information sought in the Contested Amazon Discovery (*i.e.*, financial benefits from the arrangement with Capital One) because Capital One would not necessarily have access to the full extent of that information. Regardless, there can be no dispute

that Amazon is in a greater position than Plaintiffs to access and provide information responsive to the Contested Amazon Discovery.

iv. The Remaining Factors Weigh Heavily in Plaintiffs' Favor

Amazon is without question one of the largest companies in the world and is purportedly focused on technology and data analysis. In addition to having direct knowledge of the information Plaintiffs request, Amazon arguably has the most resources of any company on the planet to gather and respond to the Contested Amazon Discovery in an efficient manner. Resolution of this dispute in Plaintiffs' favor would not result in any prejudice or undue hardship to Amazon: the parties are subject to protective and confidentiality orders, and the information sought in the Contested Amazon Discovery would undoubtedly be subject to those orders. Amazon's basis for opposing this discovery is tenuous at best, as the Contested Amazon Discovery weighs directly on [redacted] *See* Ex. G. There may be disputes later in the litigation as to the admissibility of such evidence, but that is not the standard here, and Amazon has no valid basis to oppose the responses to the Contested Amazon Discovery, including production of documents, responses to interrogatories, and presentation of a Rule 30(b)(6) thereon.

CONCLUSION

For all the reasons set forth above, Plaintiffs have satisfied their requirement of a prima facie showing that the Contested Amazon Discovery is relevant and proportionate to the needs of this case. Plaintiffs request that the Court issue an order compelling Amazon to respond to the interrogatories and requests for production, produce a competent and prepared witness on the identified topics consistent with Rule 30(b)(6), and any other relief this Court deems proper.

Dated: May 15, 2020.

Respectfully Submitted,

/s/ *Steven T. Webster*

Steven T. Webster (VSB No. 31975)
WEBSTER BOOK LLP
300 N. Washington Street, Suite 404
Alexandria, Virginia 22314
Tel: (888) 987-9991
swebster@websterbook.com

Plaintiffs' Local Counsel

Norman E. Siegel
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, MO 64112
Tel: (816) 714-7100
siegel@stuevesiegel.com

Karen Hanson Riebel
LOCKRIDGE GRINDAL NAUEN, P.L.L.P
100 Washington Avenue South, Suite 200
Minneapolis, MN 55401
Tel: (612) 339-6900
khriebel@locklaw.com

John A. Yanchunis
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel: (813) 223-5505
jyanchunis@ForThePeople.com

Plaintiffs' Co-Lead Counsel

CERTIFICATE OF SERVICE

I hereby certify that on May 15, 2020, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system, which will send notice of electronic filing to all counsel of record.

/s/ *Steven T. Webster*
Steven T. Webster (VSB No. 31975)
WEBSTER BOOK LLP